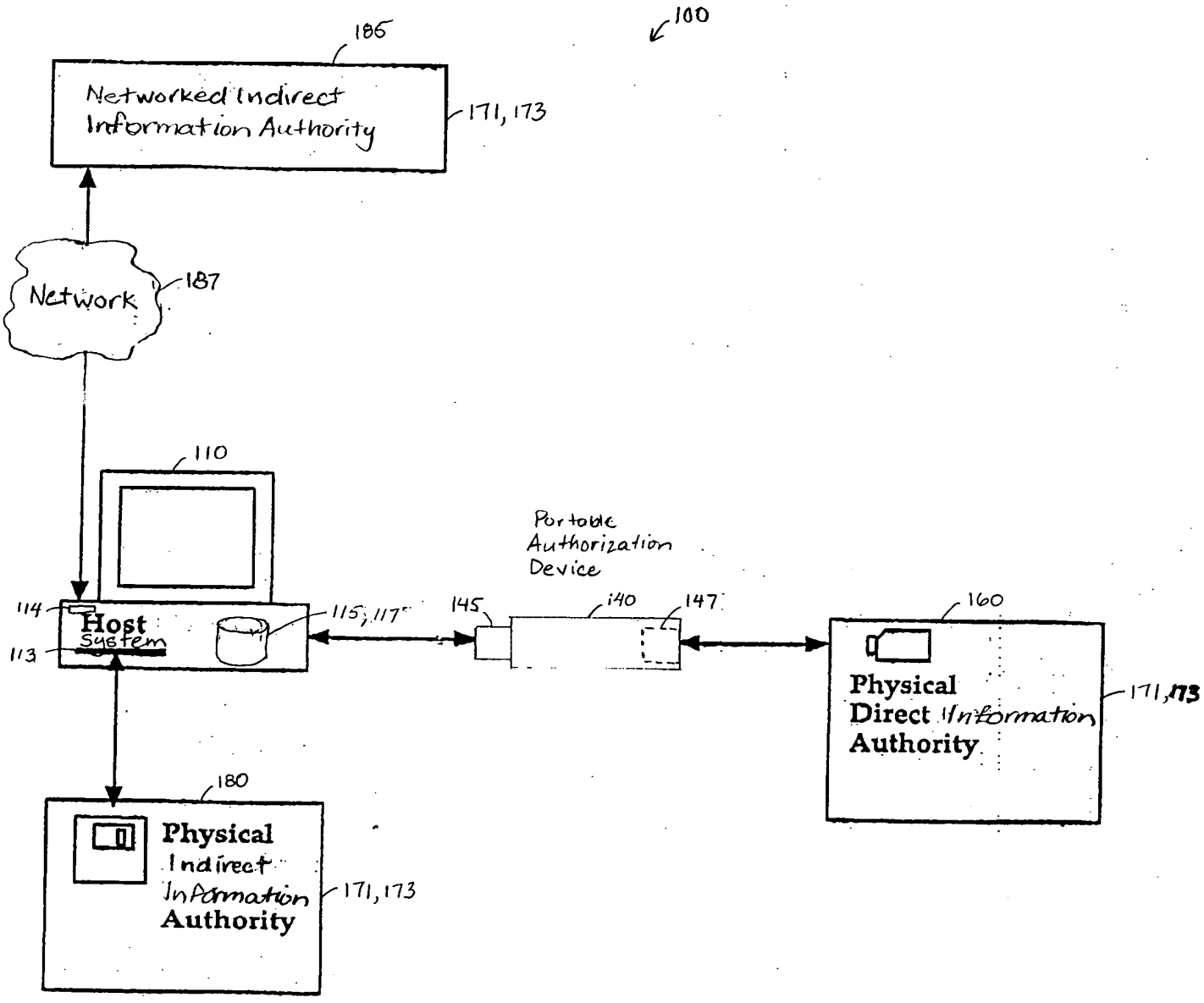
100
186
Networked Indirect Information Authority
171, 173
Network
187
110
Portable Authorization Device
114
Host System
113
115, 117
145
140
147
160
Physical Direct Information Authority
171, 173
180
Physical Indirect Information Authority
171, 173

FIG. 1

OVERALL AUTHORIZATION PROCESS

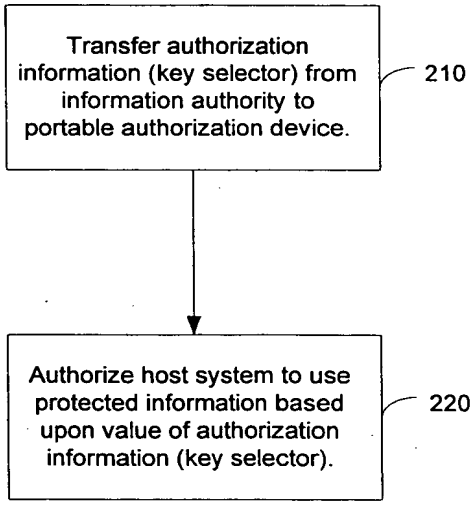

FIG. 2

PORTABLE AUTHORIZATION DEVICE

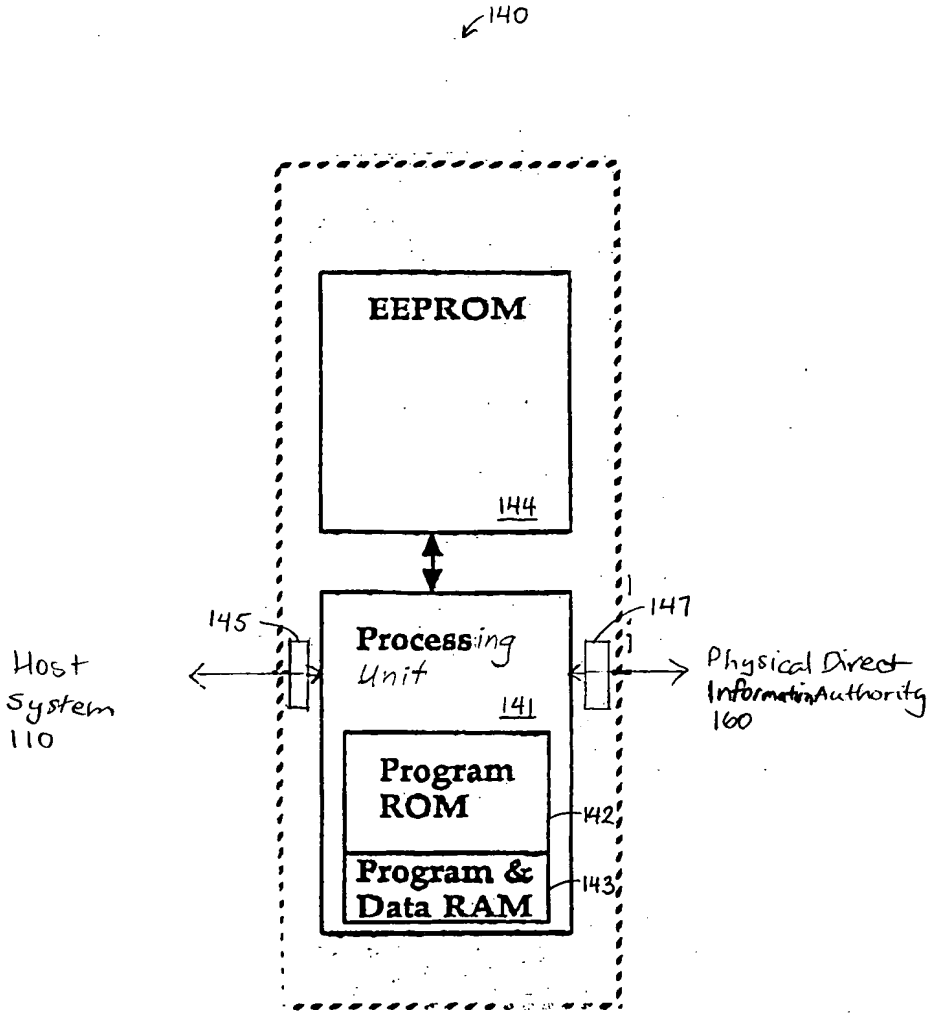

FIG. 3

FUNCTIONAL COMPONENTS OF
PORTABLE AUTHORIZATION DEVICE

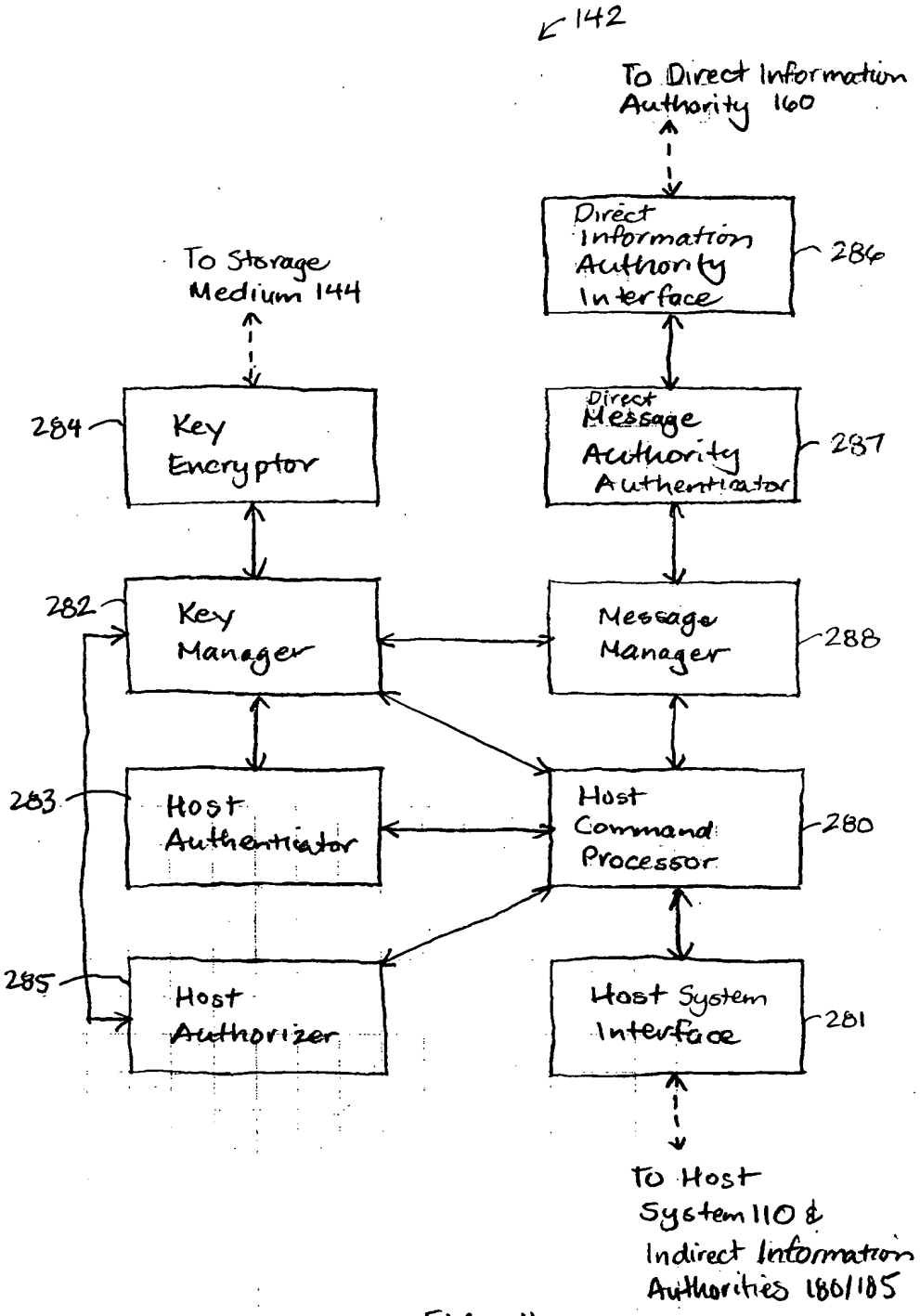

FIG. 4

PORTABLE AUTHORIZATION DEVICE
STORAGE MEDIUM

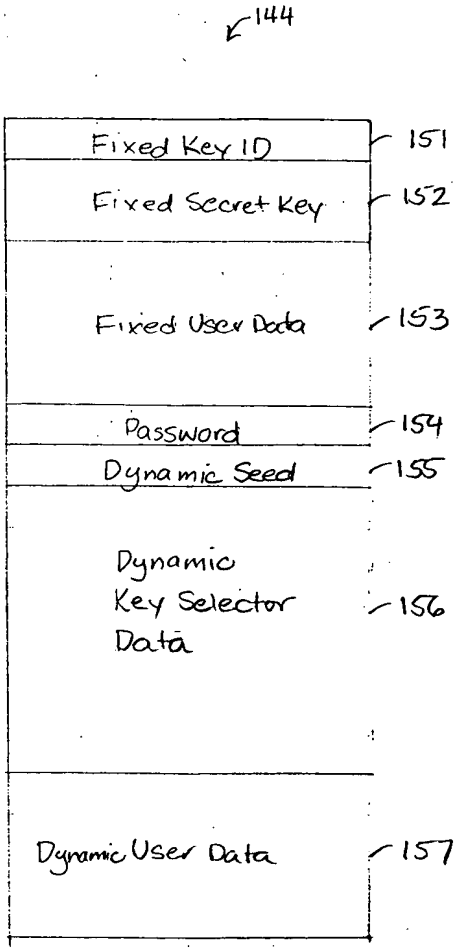

FIG. 5

FORMAT OF

DYNAMIC USER DATA

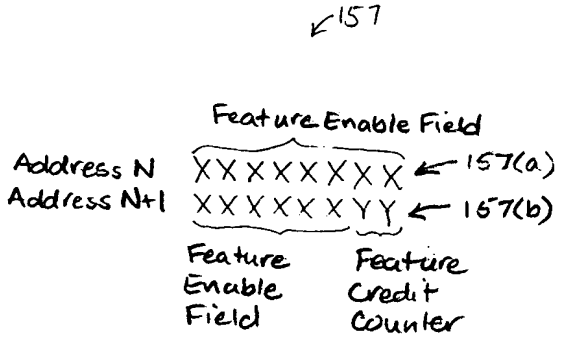

FIG. 6

PHYSICAL DIRECT

MESSAGE AUTHORITY

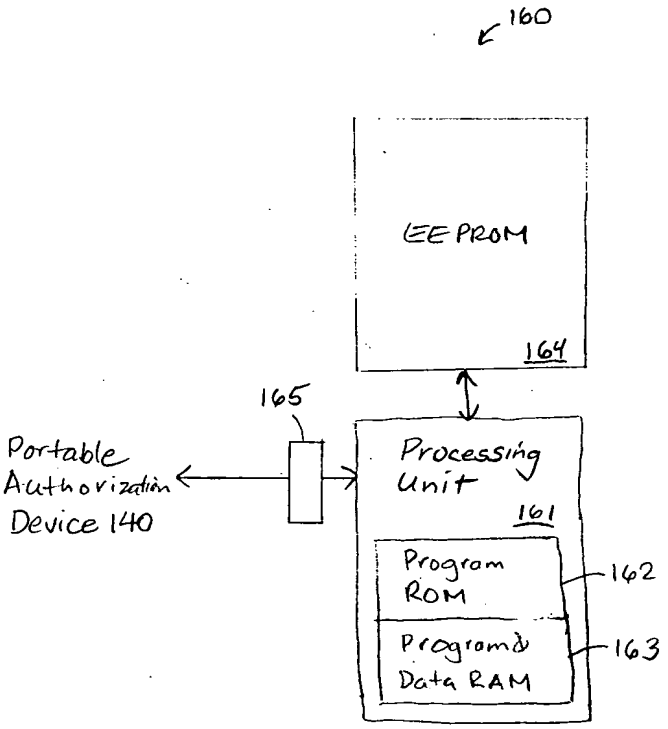

FIG. 7

PHYSICAL DIRECT
MESSAGE AUTHORITY
STORAGE MEDIUM

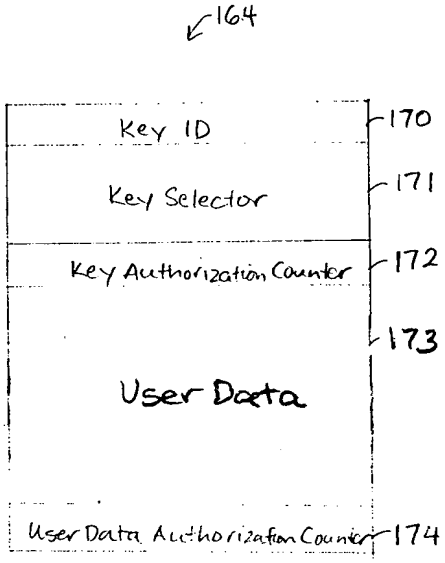

FIG. 8

KEY SELECTOR TRANSFER PROCESS

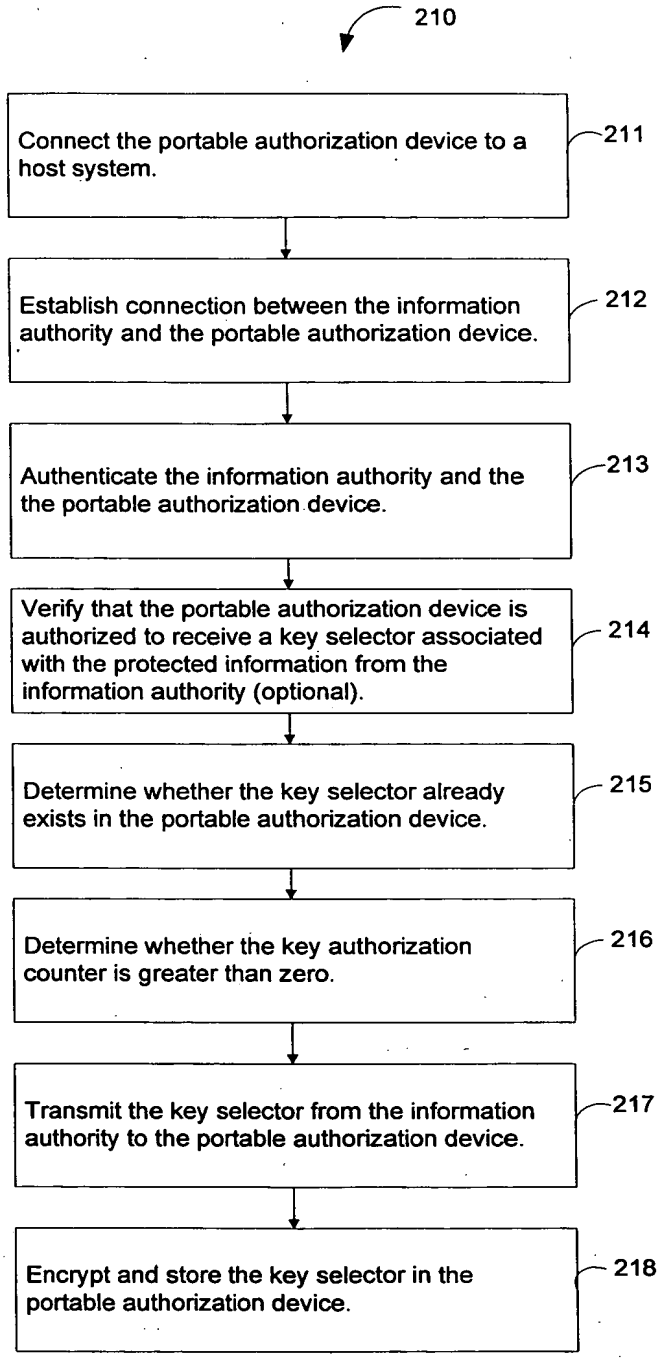

FIG. 9

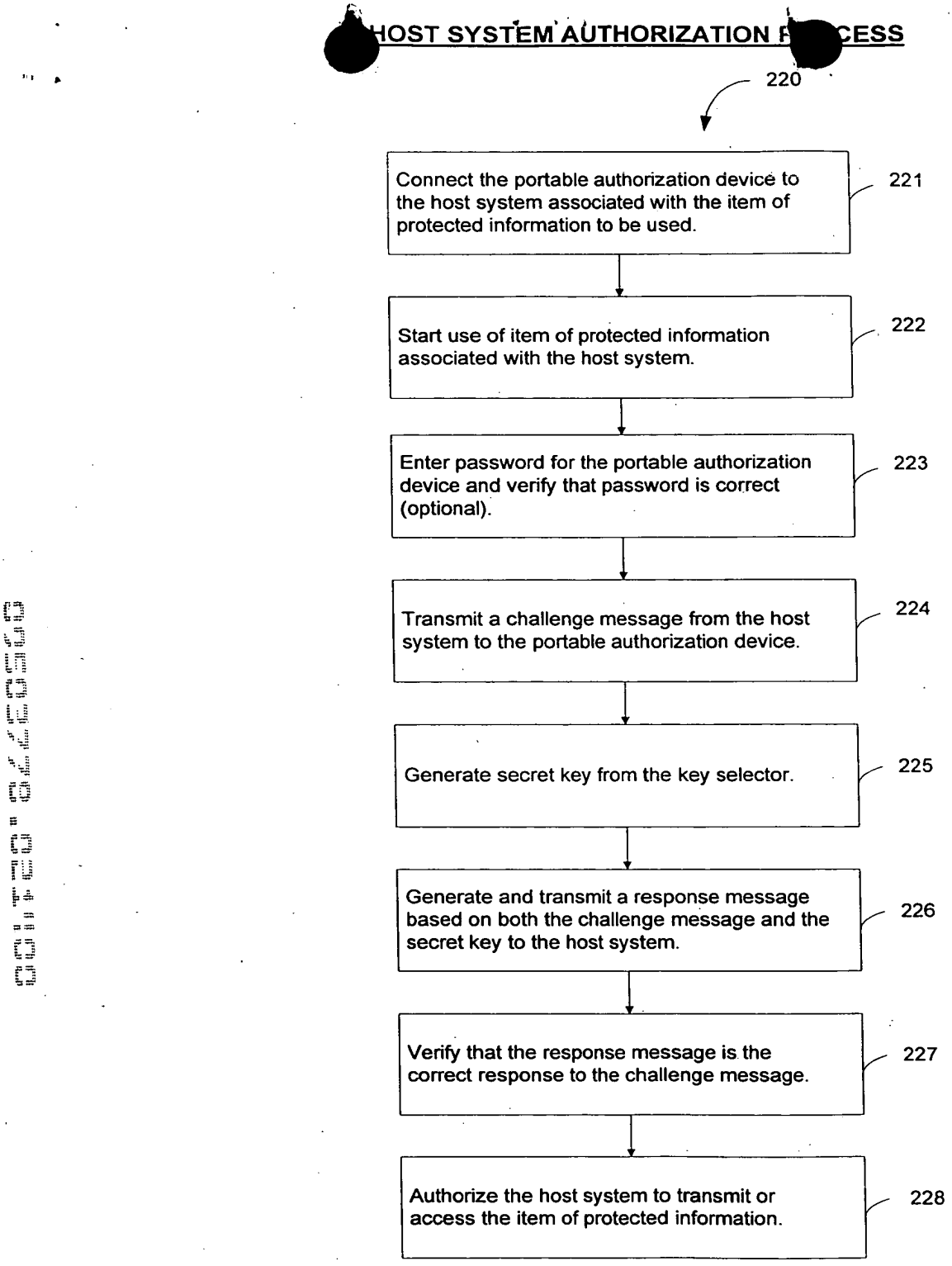
HOST SYSTEM AUTHORIZATION PROCESS
220
Connect the portable authorization device to the host system associated with the item of protected information to be used.
221
Start use of item of protected information associated with the host system.
222
Enter password for the portable authorization device and verify that password is correct (optional).
223
Transmit a challenge message from the host system to the portable authorization device.
224
Generate secret key from the key selector.
225
Generate and transmit a response message based on both the challenge message and the secret key to the host system.
226
Verify that the response message is the correct response to the challenge message.
227
Authorize the host system to transmit or access the item of protected information.
228

FIG. 10

KEY BLENDING ALGORITHM

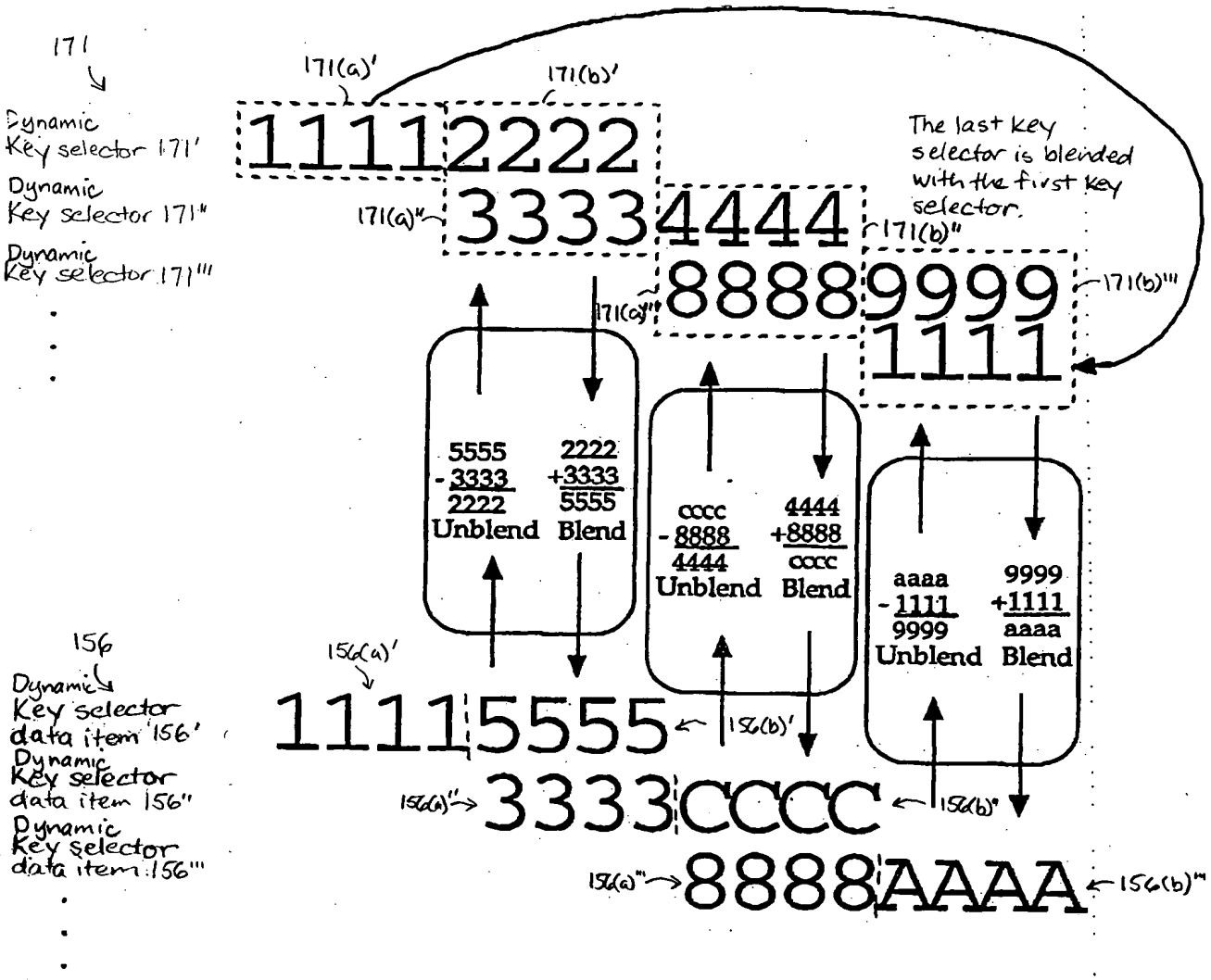

FIG. 11

KEY EXCHANGE BETWEEN TWO PORTABLE AUTHORIZATION DEVICES

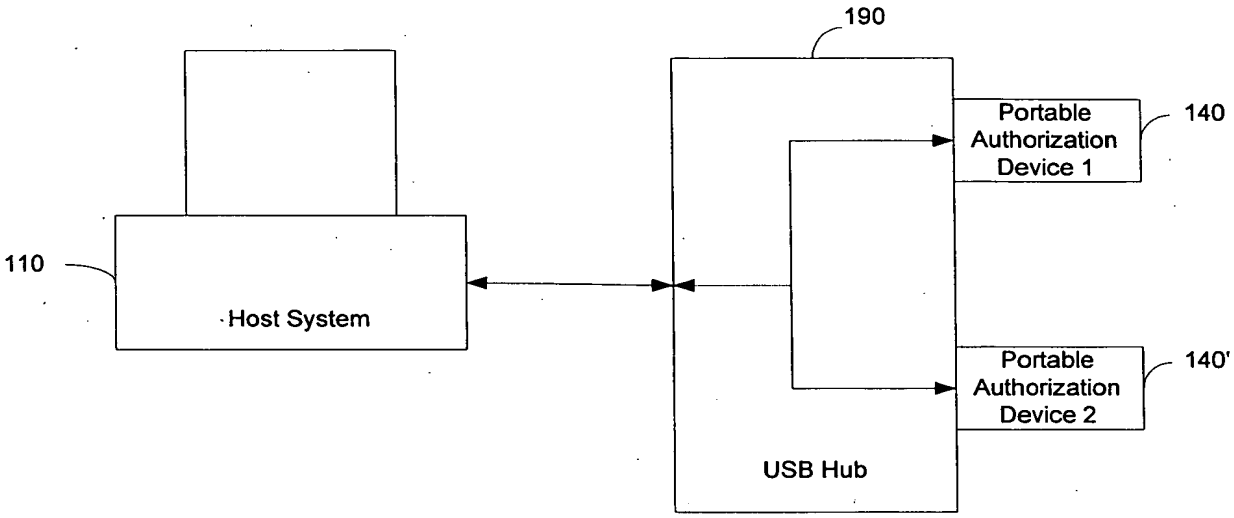

FIG. 12